

Unitary Cayley Graphs of Dedekind Domain Quotients

Colin Defant
 Department of Mathematics
 University of Florida
 United States
 cdefant@ufl.edu

Abstract

If X is a commutative ring with unity, then the unitary Cayley graph of X , denoted G_X , is defined to be the graph whose vertex set is X and whose edge set is $\{\{a, b\} : a - b \in U(X)\}$, where $U(X)$ denotes the group of units of X . When R is a Dedekind domain and I is an ideal of R such that R/I is finite and nontrivial, we refer to $G_{R/I}$ as a *generalized totient graph*. We study generalized totient graphs as generalizations of the graphs $G_{\mathbb{Z}/(n)}$, which have appeared recently in the literature, sometimes under the name *Euler totient Cayley graphs*. We begin by generalizing to Dedekind domains the arithmetic functions known as Schemmel totient functions, and we use one of these generalizations to provide a simple formula, for any positive integer m , for the number of cliques of order m in a generalized totient graph. We then proceed to determine many properties of generalized totient graphs such as their clique numbers, chromatic numbers, chromatic indices, clique domination numbers, and (in many, but not all cases) girths. We also determine the diameter of each component of a generalized totient graph. We correct one erroneous claim about the clique domination numbers of Euler totient Cayley graphs that has appeared in the literature and provide a counterexample to a second claim about the strong domination numbers of these graphs.

1 Introduction

Throughout this paper, we will let \mathbb{N} denote the set of positive integers. We will let $U(X)$ and $\text{char}(X)$ denote, respectively, the set of units and the characteristic of a ring X . We will always let R be an arbitrary Dedekind domain. For nonzero ideals I and J of R , we will make repeated use of the fact that $|R/IJ| = |R/I| \cdot |R/J|$ regardless of whether or not I and J are relatively prime ideals. Furthermore, if I factors into powers of prime ideals as $I = P_1^{\alpha_1} \cdots P_t^{\alpha_t}$, then $a + I \in U(R/I)$ if and only if $a \notin P_i$ for each $i \in \{1, \dots, t\}$. When R/I is finite, we will refer to $|R/I|$ as the index of I in R . If $I \neq (0)$ and R/I is finite and nontrivial, then we will let $Q(I)$ denote the minimum of $|R/P|$ as P ranges over all prime ideal divisors of I .

We will frequently speak of elements of certain quotient rings whose representatives have certain properties, and we will omit any reference to the fact that we could have chosen different representatives if it is clear that all representatives of a given coset either do or do not have the specific properties. For example, we may speak of the elements $a + (6) \in \mathbb{Z}/(6)$ that satisfy $2|a$. As another example, if $x \in R$, we may consider the set $\{v + (x) \in R/(x) : v + 1 + (x) \in U(R/(x))\}$. In the first example, we omit the detail that $2|a$ if and only if $2|b$ for all $b \in a + (6)$. Similarly, in the second example, we leave out the fairly obvious fact that $v + 1 + (x)$ is the same coset as $w + 1 + (x)$ for any choice of a representative w of $v + (x)$.

The well-known Euler totient function $\phi: \mathbb{N} \rightarrow \mathbb{N}$ maps a positive integer n to the number of positive integers that are less than or equal to n and relatively prime to n . In other words, $\phi(n) = |U(\mathbb{Z}/(n))|$. In 1869, V. Schemmel introduced a class of functions S_r , now known as Schemmel totient functions, which generalize the Euler totient function. For all positive integers r and n , $S_r(n)$ counts the number of positive integers $k \leq n$ such that $\gcd(k + i, n) = 1$ for all $i \in \{0, 1, \dots, r - 1\}$. Thus, $S_1 = \phi$. We will convene to let $S_0(n) = n$ for all positive integers n . For each nonnegative integer r , S_r is a multiplicative arithmetic function that satisfies

$$S_r(p^\alpha) = \begin{cases} 0, & \text{if } p \leq r; \\ p^{\alpha-1}(p - r), & \text{if } p > r \end{cases} \quad (1)$$

for all primes p and positive integers α [6]. We may consider an extension of

the Euler totient function to Dedekind domains, defining $\varphi(R/I) = |U(R/I)|$ whenever I is an ideal of R such that R/I is finite (we will use the symbol ϕ to represent the traditional Euler totient function whose domain is \mathbb{N} , and we will use φ to represent this mapping from quotients of Dedekind domains to \mathbb{Z}). Thus, $\varphi(\mathbb{Z}/(n)) = \phi(n)$ for all $n \in \mathbb{N}$. Later, we will define two classes of functions that will each serve to extend the Schemmel totient functions to Dedekind domains.

Our primary goal is to study properties of certain unitary Cayley graphs. If X is a commutative ring with unity, then the unitary Cayley graph of X , denoted G_X , is defined to be the graph whose vertex set is X and whose edge set is $\{\{a, b\} : a - b \in U(X)\}$. The unitary Cayley graphs $G_{\mathbb{Z}/(n)}$ for $n \in \mathbb{N}$ have been named “Euler totient Cayley graphs” [3, 4, 5]. Several researchers have shown that the graph $G_{\mathbb{Z}/(n)}$ contains exactly $\frac{1}{6}n\phi(n)S_2(n)$ triangles [1, 2, 3], and Manjuri and Maheswari have studied Euler totient Cayley graphs in the context of domination parameters [4, 5]. Klotz and Sander have studied, among other properties, the diameters and eigenvalues of Euler totient Cayley graphs [2], and their paper gives a list of references to other results related to these graphs.

We define a *generalized totient graph* to be a unitary Cayley graph $G_{R/I}$, where I is an ideal of the Dedekind domain R and R/I is finite and nontrivial. We seek to gain information about many of the properties of generalized totient graphs. In particular, we will use one of our two extensions of the Schemmel totient functions to give a formula, for each positive integer m , for the number of cliques of order m in a given generalized totient graph. This formula will allow us to determine the clique domination numbers of generalized totient graphs and correct an erroneous claim that Manjuri and Maheswari have made regarding this topic. We will build upon the work of Klotz and Sander, who have determined the diameters of Euler totient Cayley graphs. We end the paper with suggestions for further research and a counterexample to a claim that Manjuri and Maheswari have made regarding the strong domination numbers of Euler totient Cayley graphs.

2 Extending the Schemmel Totient Functions

Our first extension of the Schemmel totient functions is inspired by our original definition of $S_r(n)$, for any given $r, n \in \mathbb{N}$, as the number of positive integers $k \leq n$ such that $\gcd(k+i, n) = 1$ for all $i \in \{0, 1, \dots, r-1\}$. Implicit in the following definition is the fact that every Dedekind domain has a unity element, which we will denote 1. Furthermore, a positive integer k , when used to denote an element of a Dedekind domain, will be understood to represent the sum $\underbrace{1 + 1 + \dots + 1}_{k \text{ times}}$. In particular, a set such as $\{1, 2, \dots, k\}$

will denote the set $\left\{ 1, 1+1, \dots, \underbrace{1+1+\dots+1}_{k \text{ times}} \right\}$ when it is clear from context that the elements of this set are elements of the Dedekind domain.

Definition 2.1. Let I be an ideal of R such that R/I is finite. For any positive integer r , we define the set $L_r(R/I)$ by

$$L_r(R/I) = \{a + I \in R/I : a + i + I \in U(R/I) \forall i \in \{0, 1, \dots, r-1\}\}.$$

Furthermore, we define $\mathcal{S}_r(R/I)$ by $\mathcal{S}_r(R/I) = |L_r(R/I)|$.

Remark 2.1. Setting $R = \mathbb{Z}$ and $I = (n)$ in Definition 2.1 yields $\mathcal{S}_r(\mathbb{Z}/(n)) = S_r(n)$. Observe that $\mathcal{S}_r(R/R) = 1$. Also, note that $L_1(R/I) = U(R/I)$, so $\mathcal{S}_1(R/I) = |U(R/I)| = \varphi(R/I)$.

The following two theorems show that the functions \mathcal{S}_r can be evaluated using a formula similar to (1).

Theorem 2.1. *Let I and J be relatively prime nonzero ideals of R such that R/I and R/J are finite. Then $\mathcal{S}_r(R/IJ) = \mathcal{S}_r(R/I)\mathcal{S}_r(R/J)$ for all positive integers r .*

Proof. Fix some positive integer r . Consider the natural ring homomorphisms $\psi_1: R/IJ \rightarrow R/I$ and $\psi_2: R/IJ \rightarrow R/J$ defined by $\psi_1: a+IJ \mapsto a+I$ and $\psi_2: a+IJ \mapsto a+J$. Because I and J are relatively prime, we know that the function $f: R/IJ \rightarrow R/I \oplus R/J$ defined by $f: a+IJ \mapsto (a+I, a+J) = (\psi_1(a+IJ), \psi_2(a+IJ))$ is a ring isomorphism. Now, $a+IJ \in L_r(R/IJ)$ if

and only if $a + i + IJ \in U(R/IJ)$ for all $i \in \{0, 1, \dots, r-1\}$. This occurs if and only if $\psi_1(a + IJ) \in L_r(R/I)$ and $\psi_2(a + IJ) \in L_r(R/J)$, which occurs if and only if $f(a + IJ) \in L_r(R/I) \times L_r(R/J)$ (here, we use \times to denote the Cartesian product). Thus, there is a bijection between $L_r(R/IJ)$ and $L_r(R/I) \times L_r(R/J)$, so

$$\begin{aligned}\mathcal{S}_r(R/IJ) &= |L_r(R/IJ)| = |L_r(R/I) \times L_r(R/J)| \\ &= |L_r(R/I)| \cdot |L_r(R/J)| = \mathcal{S}_r(R/I) \mathcal{S}_r(R/J).\end{aligned}$$

□

Theorem 2.2. *Let P be a prime ideal of R such that R/P is finite. Let r and α be positive integers. Then*

$$\mathcal{S}_r(R/P^\alpha) = \begin{cases} |R/P|^{\alpha-1}(|R/P| - r), & \text{if } r \leq \text{char}(R/P); \\ |R/P|^{\alpha-1}(|R/P| - \text{char}(R/P)), & \text{if } r > \text{char}(R/P). \end{cases}$$

Proof. If we define a ring homomorphism $\psi: R/P^\alpha \rightarrow R/P$ by $\psi: a + P^\alpha \mapsto a + P$, then we see that $a + P^\alpha \in U(R/P^\alpha)$ if and only if $\psi(a + P^\alpha) \in U(R/P)$. More generally, $a + i + P^\alpha \in U(R/P^\alpha)$ for all $i \in \{0, 1, \dots, r-1\}$ if and only if $\psi(a + i + P^\alpha) \in U(R/P)$ for all $i \in \{0, 1, \dots, r-1\}$. Therefore, $a + P^\alpha \in L_r(R/P^\alpha)$ if and only if $\psi(a + P^\alpha) \in L_r(R/P)$. As ψ is clearly surjective and $\frac{|R/P^\alpha|}{|R/P|} = |R/P|^{\alpha-1}$, we know that ψ is a k -to-1 mapping, where $k = |R/P|^{\alpha-1}$. This shows that $|L_r(R/P^\alpha)| = |R/P|^{\alpha-1}|L_r(R/P)|$. We now show that

$$\mathcal{S}_r(R/P) = \begin{cases} |R/P| - r, & \text{if } r \leq \text{char}(R/P); \\ |R/P| - \text{char}(R/P), & \text{if } r > \text{char}(R/P). \end{cases}$$

Suppose that $r \leq \text{char}(R/P)$. Then $P, -1 + P, \dots, -(r-1) + P$ are distinct elements of R/P . Clearly, $-i + P \notin L_r(R/P)$ for all $i \in \{0, 1, \dots, r-1\}$. On the other hand, if $x + P \in (R/P) \setminus (L_r(R/P))$, then $x + i + P = P$ for some $i \in \{0, 1, \dots, r-1\}$. This then implies that $x + P = -i + P$ for some $i \in \{0, 1, \dots, r-1\}$. Thus, $(R/P) \setminus (L_r(R/P)) = \{P, -1 + P, \dots, -(r-1) + P\}$, so $\mathcal{S}_r(R/P) = |R/P| - r$.

Now suppose that $r > \text{char}(R/P)$, and write $\text{char}(R/P) = \chi$. Then $P, -1+P, \dots, -(\chi-1)+P$ are distinct elements of $(R/P) \setminus (L_r(R/P))$. Suppose that $x+P \in (R/P) \setminus (L_r(R/P))$. Then we have $x+i+P = P$ for some $i \in \{0, 1, \dots, r-1\}$. If we write $i \equiv j \pmod{\chi}$ for some $j \in \{0, 1, \dots, \chi-1\}$, then we know that $x+i+P = x+j+P = P$. This implies that $x+P \in \{P, -1+P, \dots, -(\chi-1)+P\}$. In other words, $(R/P) \setminus (L_r(R/P)) = \{P, -1+P, \dots, -(\chi-1)+P\}$, so $\mathcal{S}_r(R/P) = |R/P| - \text{char}(R/P)$. \square

Let $I = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k}$, where P_1, P_2, \dots, P_k are distinct prime ideals of R and $\alpha_1, \alpha_2, \dots, \alpha_k$ are positive integers. Then we may use Theorem

2.1 repeatedly to write $\mathcal{S}_r(R/I) = \prod_{i=1}^k \mathcal{S}_r(R/P_i^{\alpha_i})$ for any positive integer r .

Theorem 2.2 then allows us to evaluate $\mathcal{S}_r(R/P_i^{\alpha_i})$ for each positive integer $i \leq k$. Note that $\mathcal{S}_r(R/(0))$ is defined if R is finite. In this case, R must be a field (any finite integral domain is a field), so an argument similar to that used in the proof of Theorem 2.2 shows that

$$\mathcal{S}_r(R/(0)) = |R| - \min(r, \text{char}(R)).$$

We have established one extension of the Schemmel totient functions that is interesting in its own right, but we will see that the following slightly different extension will prove itself much more useful for our purposes later.

Definition 2.2. Let r be nonnegative integer. For each nonzero ideal I of R such that R/I is finite, we may define $\mathcal{S}_r(R/I)$ by the following rules:

- (a) $\mathcal{S}_r(R/R) = 1$.
- (b) If P is a prime ideal of finite index in R and α is a positive integer, then

$$\mathcal{S}_r(R/P^\alpha) = \begin{cases} |R/P|^{\alpha-1}(|R/P| - r), & \text{if } r \leq |R/P|; \\ 0, & \text{if } r > |R/P|. \end{cases}$$

- (c) If A and B are relatively prime nonzero ideals of finite index in R , then $\mathcal{S}_r(R/AB) = \mathcal{S}_r(R/A)\mathcal{S}_r(R/B)$.

Remark 2.2. First, note that we can evaluate $\mathcal{S}_r(R/I)$ for any nonzero ideal I of finite index in R by simply decomposing I into a product of powers of prime ideals and combining the given rules. Then $\mathcal{S}_r(R/I) = 0$ if and only if $Q(I) \leq r$. It is easy to see that $\mathcal{S}_0(R/I) = |R/I|$ and $\mathcal{S}_1(R/I) = \mathcal{S}_1(R/I) = \varphi(R/I)$ for any nonzero ideal I of finite index in R . Finally, note that if we set $R = \mathbb{Z}$, then $\mathcal{S}_r(\mathbb{Z}/(n)) = \mathcal{S}_r(\mathbb{Z}/(n)) = S_r(n)$ for any positive integers r and n .

3 Enumerating Cliques in Generalized Totient Graphs

Lemma 3.1. *Let I be a nonzero ideal of R such that R/I is finite and nontrivial, and let r be a positive integer. It is possible to find elements $x_1 + I, x_2 + I, \dots, x_r + I$ of R/I such that $x_i - x_j + I \in U(R/I)$ for all distinct $i, j \in \{1, 2, \dots, r\}$ if and only if $Q(I) \geq r$. Furthermore, if $Q(I) \geq r$, then, for any such choice of $x_1 + I, x_2 + I, \dots, x_r + I$, there are exactly $\mathcal{S}_r(R/I)$ elements $w + I$ of R/I that satisfy $w - x_i + I \in U(R/I)$ for all $i \in \{1, 2, \dots, r\}$.*

Proof. First, by way of contradiction, suppose that $Q(I) < r$ and that $x_1 + I, x_2 + I, \dots, x_r + I$ are elements of R/I such that $x_i - x_j + I \in U(R/I)$ for all distinct $i, j \in \{1, 2, \dots, r\}$. As $Q(I) < r$, there must be some prime ideal divisor P of I such that $|R/P| < r$. By the Pigeonhole Principle, we must have $x_i + P = x_j + P$ for some distinct $i, j \in \{1, 2, \dots, r\}$. However, this is a contradiction because it implies that $x_i - x_j \in P$, which then implies that $x_i - x_j + I \notin U(R/I)$.

Now, suppose $Q(I) \geq r$. Let us write $I = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_s^{\alpha_s}$, where P_1, P_2, \dots, P_s are distinct prime ideals of R and $\alpha_1, \alpha_2, \dots, \alpha_s$ are positive integers. For each positive integer $v \leq s$, we may write $|R/P_v| = m_v \geq r$ and $R/P_v = \{t_{v,1} + P_v, t_{v,2} + P_v, \dots, t_{v,m_v} + P_v\}$. For each positive integer $i \leq r$, the Chinese Remainder Theorem guarantees that it is possible to find some $x_i \in R$ such that $x_i + P_v = t_{v,i} + P_v$ for all positive integers $v \leq s$. Then, for all distinct $i, j \in \{1, 2, \dots, r\}$ and all $v \in \{1, 2, \dots, s\}$, we have $x_i - x_j + P_v = t_{v,i} - t_{v,j} + P_v \neq P_v$, so $x_i - x_j \notin P_v$. This means that $x_i - x_j + I \in U(R/I)$ for all distinct $i, j \in \{1, 2, \dots, r\}$.

Finally, suppose that $Q(I) \geq r$ and that $x_1+I, x_2+I, \dots, x_r+I$ satisfy $x_i - x_j + I \in U(R/I)$ for all distinct $i, j \in \{1, 2, \dots, r\}$. For each $j \in \{1, 2, \dots, s\}$, let N_j be the set of elements $a + P_j^{\alpha_j}$ of $R/P_j^{\alpha_j}$ such that $a - x_i \notin P_j$ for all $i \in \{1, 2, \dots, r\}$ (observe that the choices of a and x_i as representatives of their cosets do not affect whether or not $a - x_i \in P_j$ because $P_j \supseteq P_j^{\alpha_j} \supseteq I$). By the Chinese Remainder Theorem, any element $w + I$ of R/I is uniquely determined by the cosets of the ideals $P_1^{\alpha_1}, P_2^{\alpha_2}, \dots, P_s^{\alpha_s}$ that contain the representative w . Therefore, the number of ways to choose an element $w + I$ of R/I that satisfies $w - x_i + I \in U(R/I)$ for all $i \in \{1, 2, \dots, r\}$ is equal to $\prod_{j=1}^s |N_j|$. Fix $j \in \{1, 2, \dots, s\}$, and consider the natural homomorphism $\psi: R/P_j^{\alpha_j} \rightarrow R/P_j$ given by $a + P_j^{\alpha_j} \mapsto a + P_j$. We know that ψ is a k -to-1 mapping, where $k = |R/P_j|^{\alpha_j-1}$. An element A of $R/P_j^{\alpha_j}$ is in N_j if and only if $\psi(A) \neq x_i + P_j$ for all $i \in \{1, 2, \dots, r\}$. In other words, N_j is the preimage of the set $B = (R/P_j) \setminus \{x_1 + P_j, x_2 + P_j, \dots, x_r + P_j\}$ under ψ . Hence,

$$|N_j| = |R/P_j|^{\alpha_j-1} |B| = |R/P_j|^{\alpha_j-1} (|R/P_j| - r) = \mathcal{S}_r(R/P_j^{\alpha_j}).$$

Using Definition 2.2, we see that the number of elements $w + I$ of R/I that satisfy $w - x_i + I \in U(R/I)$ for all $i \in \{1, 2, \dots, r\}$ is

$$\prod_{j=1}^s |N_j| = \prod_{j=1}^s \mathcal{S}_r(R/P_j^{\alpha_j}) = \mathcal{S}_r(R/I).$$

□

We now prove our central result, which will prove itself quite useful in the next section. Recall the definition of a generalized totient graph. From now on, we will always let I denote a nonzero ideal of the Dedekind domain R such that R/I is finite and nontrivial.

Theorem 3.1. *For any positive integer m , the number of cliques of order m in the graph $G_{R/I}$ is given by the expression*

$$\prod_{k=1}^m \frac{\mathcal{S}_{k-1}(R/I)}{k}.$$

Proof. The proof is by induction on m . The case $m = 1$ is trivial because $\mathcal{S}_0(R/I) = |R/I|$, which is the number of vertices of $G_{R/I}$.

Now, suppose that $m > 1$ and that there are exactly $\prod_{k=1}^{m-1} \frac{\mathcal{S}_{k-1}(R/I)}{k}$ cliques of order $m - 1$ in $G_{R/I}$. If $\prod_{k=1}^{m-1} \frac{\mathcal{S}_{k-1}(R/I)}{k} = 0$, then there are no cliques of order m in $G_{R/I}$ because there are no cliques of order $m - 1$ in $G_{R/I}$. Hence, if $\prod_{k=1}^{m-1} \frac{\mathcal{S}_{k-1}(R/I)}{k} = 0$, then we are done because

$$\prod_{k=1}^m \frac{\mathcal{S}_{k-1}(R/I)}{k} = \frac{\mathcal{S}_{m-1}(R/I)}{m} \prod_{k=1}^{m-1} \frac{\mathcal{S}_{k-1}(R/I)}{k} = 0.$$

Therefore, let us assume that there is at least one clique of order $m - 1$ in $G_{R/I}$. Choose one of these cliques, and call it D . We wish to know the number of ways that we may extend D to a clique of order m within $G_{R/I}$ by annexing one additional vertex of $G_{R/I}$ to D . In other words, we wish to know how many vertices of $G_{R/I}$ are adjacent to every vertex in D . Let the vertices in D be $x_1 + I, x_2 + I, \dots, x_{m-1} + I$. Then $x_i - x_j + I \in U(R/I)$ for all distinct $i, j \in \{1, 2, \dots, m-1\}$ because D is a clique. Therefore, by Lemma 3.1, there are exactly $\mathcal{S}_{m-1}(R/I)$ elements $w + I$ of R/I that satisfy $w - x_i + I \in U(R/I)$ for all $i \in \{1, 2, \dots, m-1\}$. In other words, there are exactly $\mathcal{S}_{m-1}(R/I)$ vertices of $G_{R/I}$ that we may annex to D to make a clique of order m . Hence, to find the number of cliques of order m in $G_{R/I}$, we simply multiply $\prod_{k=1}^{m-1} \frac{\mathcal{S}_{k-1}(R/I)}{k}$ (the number of ways we could have chosen D) by $\mathcal{S}_{m-1}(R/I)$. However, we must then divide this number by m because we will have counted each clique of order m a total of m times (because there are m subcliques of order $m - 1$ in every clique of order m). Hence, the number of cliques of order m in $G_{R/I}$ is

$$\frac{\mathcal{S}_{m-1}(R/I)}{m} \prod_{k=1}^{m-1} \frac{\mathcal{S}_{k-1}(R/I)}{k} = \prod_{k=1}^m \frac{\mathcal{S}_{k-1}(R/I)}{k}.$$

□

Corollary 3.1. *Let m and n be positive integers with $n > 1$. The number of cliques of order m in the Euler totient Cayley graph $G_{\mathbb{Z}/(n)}$ is $\prod_{k=1}^m \frac{S_{k-1}(n)}{k}$.*

Observe that if we set $m = 3$ in Corollary 3.1, we recover the previously-discovered formula $\frac{1}{6}n\phi(n)S_2(n)$ for the number of triangles in $G_{\mathbb{Z}/(n)}$. Before proceeding to uncover some additional properties of generalized totient graphs, we pause to note an interesting divisibility relationship that arises as a corollary of Theorem 3.1.

Corollary 3.2. *For any positive integer m , we have*

$$m! \mid \prod_{k=1}^m S_{k-1}(R/I).$$

4 Other Properties of Generalized Totient Graphs

For any graph G , we will let $\chi(G)$ and $\chi'(G)$ denote the chromatic number and the chromatic index of G , respectively. We will let $g(G)$, $d(G)$, $\Delta(G)$, and $\omega(G)$ denote, respectively, the girth, diameter, maximum degree, and clique number of a graph G . A set D of vertices of a graph G is said to dominate G if every vertex in G is either in D or is adjacent to at least one element of D . The clique domination number $\gamma_{cl}(G)$ of a graph G is the smallest positive integer such that there exists a clique of G of order $\gamma_{cl}(G)$ that dominates G (provided some dominating clique exists).

We will continue to let I denote a nonzero ideal of the Dedekind domain R such that R/I is both finite and nontrivial. We begin with a fairly basic result concerning unitary Cayley graphs of commutative rings with unity. A symmetric graph is a graph G such that if A, B, C, D are vertices of G with A adjacent to B and C adjacent to D , then there exists an automorphism of G that maps A to C and maps B to D .

Theorem 4.1. *Let X be a commutative ring with unity. The unitary Cayley graph G_X is symmetric and $\varphi(X)$ -regular, where $\varphi(X) = |U(X)|$.*

Proof. Choose some $A, B, C, D \in X$ such that A is adjacent to B and C is adjacent to D . Define a function $F: X \rightarrow X$ by

$$F(Z) = C - (A - Z)(C - D)(A - B)^{-1}.$$

Observe that $F(A) = C$ and $F(B) = D$. It is straightforward to see that F is a bijection because $(A - B)$ and $(C - D)$ are units in X . Now, let Y and Z be any adjacent vertices in G_X . It follows from the fact that $Y - Z$, $A - B$, and $C - D$ are all units in X that $F(Y) - F(Z) = (Y - Z)(C - D)(A - B)^{-1} \in U(X)$. Hence, $F(Y)$ and $F(Z)$ are adjacent. Similarly, F maps nonadjacent vertices to nonadjacent vertices. This shows that F is an automorphism, so G_X is symmetric. As any symmetric graph is regular and the degree of the vertex 0 is $\varphi(X)$, we see that G_X is $\varphi(X)$ -regular. \square

Theorem 4.2. *The generalized totient graph $G_{R/I}$ is bipartite if and only if $Q(I) = 2$.*

Proof. Suppose that $Q(I) = 2$. Then there exists some prime ideal divisor P of I such that $|R/P| = 2$. If $a, b \in P$, then $a - b \in P$, so $a + I$ and $b + I$ are not adjacent in $G_{R/I}$. On the other hand, if $a \notin P$ and $b \notin P$, then $a + P = b + P$. This implies that $a - b \in P$, so $a + I$ and $b + I$ are not adjacent in $G_{R/I}$. Therefore, we may partition the set of vertices of $G_{R/I}$ into subsets A_0 and A_1 defined by $A_0 = \{a + I \in R/I : a \in P\}$ and $A_1 = \{a + I \in R/I : a \notin P\}$ so that no two vertices of the same subset are adjacent.

Conversely, suppose that $Q(I) \neq 2$. Because $Q(I)$ must be an integer larger than 1, we have $Q(I) \geq 3$. Using Theorem 3.1, we find that the number of cliques of order 3 in $G_{R/I}$ is $\prod_{k=1}^3 \frac{\mathcal{S}_{k-1}(R/I)}{k}$. As noted in Remark 2.2, $\mathcal{S}_r(R/I) = 0$ if and only if $Q(I) \leq r$. Hence, $\prod_{k=1}^3 \frac{\mathcal{S}_{k-1}(R/I)}{k} \neq 0$, so there is at least one triangle in $G_{R/I}$. This implies that $G_{R/I}$ cannot be bipartite. \square

In the proof of Theorem 4.2, we used the fact that $G_{R/I}$ contains a clique of order 3 whenever $Q(I) \geq 3$. It turns out that this fact generalizes, as the following theorem shows.

Theorem 4.3. *The generalized totient graph $G_{R/I}$ satisfies*

$$\omega(G_{R/I}) = \chi(G_{R/I}) = Q(I).$$

Proof. We make use of the fact that $\mathcal{S}_r(R/I) = 0$ if and only if $Q(I) \leq r$ to see that $\prod_{k=1}^{Q(I)} \frac{\mathcal{S}_{k-1}(R/I)}{k} > 0$. Thus, by Theorem 3.1, there is at least one clique of $G_{R/I}$ of order $Q(I)$. Furthermore, there is no clique of $G_{R/I}$ of order m for any $m > Q(I)$ because $\mathcal{S}_{m-1}(R/I) = 0$ for all $m > Q(I)$. Using the trivial fact that $\omega(G_{R/I}) \leq \chi(G_{R/I})$, we see that it suffices, in order to complete the proof, to exhibit a proper coloring of the vertices of $G_{R/I}$ with $Q(I)$ colors. To do so, let P be a prime ideal divisor of I such that $|R/P| = Q(I)$ (such a prime ideal divisor is guaranteed to exist by the definition of $Q(I)$). Then, simply color the vertices of $G_{R/I}$ so that two vertices $a + I$ and $b + I$ are given the same color if and only if $a - b \in P$. This coloring clearly has the desired properties, so the proof is complete. \square

Before we attempt to determine the chromatic indices of generalized totient graphs, we need two quick lemmata that should make the proof of the following theorem relatively painless.

Lemma 4.1. *Let m be a positive even integer, and let G be a simple graph with the following properties:*

- (a) *It is possible to partition the vertices of G into m sets A_1, A_2, \dots, A_m , all of the same cardinality, such that no two vertices in the same set A_i are adjacent.*
- (b) *For all distinct $i, j, k \in \{1, 2, \dots, m\}$ and any $v \in A_i$, v is adjacent to exactly as many vertices in A_j as it is to vertices in A_k .*

Then $\chi'(G) = \Delta(G)$.

Proof. Because of the trivial inequality $\chi'(G) \geq \Delta(G)$, it suffices to exhibit a proper edge-coloring of G with $\Delta(G)$ colors. Let V be a vertex of G of degree $\Delta(G)$. Without loss of generality, we may assume that $V \in A_m$. Suppose V

is adjacent to exactly t vertices in A_1 . Then, by property (b), V is adjacent to exactly t vertices in A_i for each $i \in \{1, 2, \dots, m-1\}$. As V is not adjacent to any vertices in A_m , we see that $\Delta(G) = (m-1)t$. Hence, we may label our $\Delta(G)$ colors $C_{\mu,\lambda}$, where μ ranges over the set $\{1, 2, \dots, m-1\}$ and λ ranges over the set $\{1, 2, \dots, t\}$. Now, let b_1, b_2, \dots, b_m be the vertices of the complete graph K_m . It is well-known that, because m is even, it is possible to properly color the edges of K_m with $m-1$ colors, say c_1, c_2, \dots, c_{m-1} . For any distinct $i, j \in \{1, 2, \dots, m\}$, let $f(i, j)$ be the unique positive integer less than m such that $c_{f(i,j)}$ is the color used to color the edge connecting b_i and b_j .

We now describe how to color the edges of G . For any distinct $i, j \in \{1, 2, \dots, m\}$, let $H_{i,j}$ be the subgraph of G induced by the vertices in $A_i \cup A_j$. Every such graph $H_{i,j}$ is clearly a bipartite graph with maximum degree at most t . Hence, König's Line Coloring Theorem implies that, for any distinct $i, j \in \{1, 2, \dots, m\}$, it is possible to properly color the edges of $H_{i,j}$ with only the colors in the set $\{C_{f(i,j),\lambda} : \lambda \in \{1, 2, \dots, t\}\}$. Doing so for all subgraphs $H_{i,j}$ yields a proper coloring of G with $\Delta(G)$ colors. \square

Lemma 4.2. *Let δ be a positive integer. Any δ -regular simple graph G with an odd number of vertices has chromatic index $\chi'(G) = \delta + 1$.*

Proof. Let G be a δ -regular simple graph with m vertices, where m is an odd positive integer. If there exists a proper edge-coloring of G with s colors, then no color can be used more than $\lfloor \frac{m}{2} \rfloor$ times. This then implies that the number of edges of G cannot exceed $s \lfloor \frac{m}{2} \rfloor$. As the number of edges of G is $\frac{1}{2}m\delta$, we have

$$\frac{1}{2}m\delta \leq s \left\lfloor \frac{m}{2} \right\rfloor = s \frac{m-1}{2},$$

so $s \geq \delta \frac{m}{m-1} > \delta$. By the definition of χ' , there exists a proper edge-coloring of G with $\chi'(G)$ colors, so $\chi'(G) > \delta$. Then, because Vizing's Theorem implies that $\chi'(G) \leq \delta + 1$, we conclude that $\chi'(G) = \delta + 1$. \square

Theorem 4.4. *If I has a prime ideal divisor whose index in R is a power of 2, then $\chi'(G_{R/I}) = \varphi(R/I)$. Otherwise, $\chi'(G_{R/I}) = \varphi(R/I) + 1$.*

Proof. First, suppose I has a prime ideal divisor P such that $|R/P| = 2^k = m$ for some positive integer k . Let $R/P = \{a_1 + P, a_2 + P, \dots, a_m + P\}$. Let us write $I = P^\alpha J$, where α is a positive integer and $J \not\subseteq P$. Define a homomorphism $\psi: R/I \rightarrow R/P$ by $\psi: a + I \mapsto a + P$, and, for each positive integer $i \leq m$, let $A_i = \psi^{-1}(a_i + P) = \{a + I \in R/I : a - a_i \in P\}$. The sets A_i , all of which have the same cardinality, partition the vertices of $G_{R/I}$. Furthermore, no two vertices in the same set A_i are adjacent. Hence, $G_{R/I}$ satisfies property (a) of Lemma 4.1. Now, fix some distinct $i, j \in \{1, 2, \dots, m\}$ and some vertex $v + I \in A_i$. There are exactly $m^{\alpha-1}$ elements $w + P^\alpha$ of R/P^α such that $w - a_j \in P$, and every one of those elements satisfies $w - v \notin P$ because $v - a_i \in P$ and $a_i - a_j \notin P$. Also, if we view the set $v + U(R/J) = \{v + s + J \in R/J : s + J \in U(R/J)\}$ as a coset of the subgroup $U(R/J)$ of R/J , then we see that there are exactly $\varphi(R/J)$ elements $w + J$ of R/J such that $w - v + J \in U(R/J)$. A vertex $w + I$ of $G_{R/I}$ is an element of A_j that is adjacent to $v + I$ if and only if $w - a_j \in P$, $w - v \notin P$, and $w - v + J \in U(R/J)$. Because $R/I \cong R/P^\alpha \oplus R/J$, we see that there are exactly $m^{\alpha-1} \varphi(R/J)$ such vertices. This number does not depend on the choice of j (so long as $j \neq i$), so $G_{R/I}$ satisfies property (b) of Lemma 4.1. Therefore, by Theorem 4.1 and Lemma 4.1, $\chi'(G_{R/I}) = \Delta(G_{R/I}) = \varphi(R/I)$.

Now, suppose that I does not have a prime ideal divisor whose index in R is a power of 2. Let us write $I = Q_1^{\alpha_1} Q_2^{\alpha_2} \cdots Q_t^{\alpha_t}$, where Q_1, Q_2, \dots, Q_t are prime ideals of R and $\alpha_1, \alpha_2, \dots, \alpha_t$ are positive integers. For each positive integer $i \leq t$, R/Q_i is a finite field, so $|R/Q_i|$ must be a power of an odd prime. Hence, $|R/I| = \prod_{i=1}^t |R/Q_i|^{\alpha_i}$ is odd, so $G_{R/I}$ has an odd number of vertices. Using Theorem 4.1 and Lemma 4.2, we conclude that $\chi'(G_{R/I}) = \varphi(R/I) + 1$. \square

In the following theorem, we determine when $\gamma_{cl}(G_{R/I})$ exists, and we find the value of $\gamma_{cl}(G_{R/I})$ when it does exist. Manjuri and Maheswari made the claim that if n is a composite odd integer, then $\gamma_{cl}(G_{\mathbb{Z}/(n)})$ exists if and only if n has 2 or fewer distinct prime factors [4]. However, setting $R = \mathbb{Z}$ and $I = (n)$ in the following theorem shows that their claim is false. We let $\lambda(I)$ denote the number of distinct prime ideal divisors of I .

Theorem 4.5. *If I is a prime ideal, then $\gamma_{cl}(G_{R/I}) = 1$. If I is not a prime ideal and $Q(I) > \lambda(I)$, then $\gamma_{cl}(G_{R/I}) = \lambda(I) + 1$. If I is not prime and*

$Q(I) \leq \lambda(I)$, then $\gamma_{cl}(G_{R/I})$ does not exist. Furthermore, if $\gamma_{cl}(G_{R/I})$ exists, then every clique of $G_{R/I}$ of order $\gamma_{cl}(G_{R/I})$ dominates $G_{R/I}$.

Proof. Because R is a Dedekind domain, R/I is a field if and only if I is prime. In other words, $G_{R/I}$ is complete if and only if I is prime. Therefore, if I is prime, any single vertex of $G_{R/I}$ forms a dominating clique. Now, suppose I is not prime. Let $P_1, P_2, \dots, P_{\lambda(I)}$ be the prime ideal divisors of I , and assume that $C = \{v_1 + I, v_2 + I, \dots, v_t + I\}$ is a clique of $G_{R/I}$ of order $t \leq \lambda(I)$. If $t = 1$, then we know we may find some vertex of $G_{R/I}$ other than $v_1 + I$ that is not adjacent to $v_1 + I$ because $G_{R/I}$ is regular and not complete. Therefore, no clique of order 1 dominates $G_{R/I}$. Suppose $t > 1$. By the Chinese Remainder Theorem, we know that we may find some $z + I \in R/I$ such that $z + P_i = v_i + P_i$ for all positive integers $i \leq t$. This implies that $z + I$ is not adjacent to any element of C . Then, because any vertex in C is adjacent to all other vertices in C , $z + I$ cannot be in C . Thus, C does not dominate $G_{R/I}$, so we conclude that no clique of order $t \leq \lambda(I)$ can dominate $G_{R/I}$ when I is not prime.

Now, suppose I is not prime and $Q(I) > \lambda(I)$. Again, let $P_1, P_2, \dots, P_{\lambda(I)}$ be the prime ideal divisors of I . There exists at least one clique of $G_{R/I}$ of order $\lambda(I) + 1$ because $\lambda(I) + 1 \leq Q(I) = \omega(G_{R/I})$ (by Theorem 4.3), so we may let D be an arbitrary clique of $G_{R/I}$ of order $\lambda(I) + 1$. We will show that D dominates $G_{R/I}$. Suppose, for the sake of finding a contradiction, that there is some vertex $z + I \in R/I$ that is not adjacent to any of the vertices of D . By the Pigeonhole Principle, there must be some prime ideal divisor P_i of I and some distinct $a + I, b + I \in D$ such that $z - a \in P_i$ and $z - b \in P_i$. Then $a - b \in P_i$, which contradicts the fact that $a - b + I \in U(R/I)$ because D is a clique.

Finally, suppose I is not prime and $Q(I) \leq \lambda(I)$. Because the clique number of $G_{R/I}$ is $Q(I)$ by Theorem 4.3, we see that there are no cliques of order larger than $\lambda(I)$. Thus, no clique of $G_{R/I}$ can dominate $G_{R/I}$, so $\gamma_{cl}(G_{R/I})$ does not exist. \square

If $Q(I) \geq 3$, then $g(G_{R/I}) = 3$ because $\omega(G_{R/I}) \geq 3$ by Theorem 4.3. On the other hand, if $Q(I) = 2$, then Theorem 4.2 implies that $G_{R/I}$ contains no odd cycles. Therefore, if $Q(I) = 2$, then $g(G_{R/I}) \geq 4$. The following theorem

shows that $g(G_{R/I}) \leq 4$ for many (but not all) generalized totient graphs $G_{R/I}$.

Theorem 4.6. *Let $P = (p)$ be a prime principal ideal of R , and let J be an ideal of R that is not contained in P . Let $I = P^\alpha J$, where α is a positive integer. If $\alpha > 1$ or if $p - 1, p + 1 \notin J$, then $G_{R/I}$ has a cycle of length 4.*

Proof. Suppose $\alpha > 1$ or $p - 1, p + 1 \notin J$. Let y be an element of J that is not in P . Consider the vertices $V_1 = I$, $V_2 = p^2 - y + I$, $V_3 = p^2 + p + I$, and $V_4 = p - y + I$. Suppose V_1 and V_2 are not adjacent. If $p^2 - y \in P$, then $y = p^2 - (p^2 - y) \in P$, which contradicts our choice of y . Therefore, $p^2 - y \in Q$ for some prime ideal divisor Q of J . This implies that $p^2 = p^2 - y + y \in Q$ because $y \in J \subseteq Q$. We then have $P^2 = (p^2) \subseteq Q$, so Q is a prime ideal divisor of P^2 . As P is a prime ideal, we must have $P = Q \supseteq J$, which contradicts our hypothesis that $J \not\subseteq P$. Hence, V_1 and V_2 are adjacent. Similar arguments show that V_2 is adjacent to V_3 , V_3 is adjacent to V_4 , and V_4 is adjacent to V_1 . Therefore, if V_1, V_2, V_3 , and V_4 are all distinct, they form a cycle of length 4. We know that $V_1 \neq V_2$, $V_2 \neq V_3$, $V_3 \neq V_4$, and $V_4 \neq V_1$ because no vertex of $G_{R/I}$ can be adjacent to itself. Hence, it suffices to show that $V_1 \neq V_3$ and $V_2 \neq V_4$.

Suppose $\alpha > 1$. As $1 \notin P$ and $P^{\alpha-1} \subseteq P$, $p - 1 \notin P^{\alpha-1}$. This implies that $p^2 - p \notin P^\alpha$, so $(p^2 - y) - (p - y) = p^2 - p \notin I$. Thus, $V_2 \neq V_4$. Similarly, $p^2 + p \notin I$, so $V_1 \neq V_3$.

Suppose, now, that $\alpha = 1$. Then $p - 1 \notin J$, so $(p^2 - y) - (p - y) = p(p - 1) \notin PJ = I$. This shows that $V_2 \neq V_4$. Similarly, $p + 1 \notin J$, so $p^2 + p = p(p + 1) \notin PJ = I$. This implies that $V_1 \neq V_3$. \square

Corollary 4.1. *If $n \geq 3$ is an integer, then $g(G_{\mathbb{Z}/(n)}) = \begin{cases} 3, & \text{if } 2 \nmid n; \\ 4, & \text{if } 2 \mid n \neq 6; \\ 6, & \text{if } n = 6. \end{cases}$*

Proof. If $2 \nmid n$, then $g(G_{\mathbb{Z}/(n)}) = 3$ because $Q((n)) \geq 3$. It is easy to see that $g(G_{\mathbb{Z}/(6)}) = 6$ because $G_{\mathbb{Z}/(6)}$ is a cycle of length 6. Assume, now, that $2 \mid n$ and $n \neq 6$. Because $2 \mid n$, $g(G_{\mathbb{Z}/(n)}) \neq 3$. Write $n = 2^\alpha m$ for some positive integers m and α with m odd. Setting $p = 2$ and $J = (m)$ in Theorem 4.6 shows that there is a cycle of length 4 in $G_{\mathbb{Z}/(n)}$, so $g(G_{\mathbb{Z}/(n)}) = 4$. \square

5 Diameters and Disconnectedness

Klotz and Sander have determined the diameters of all Euler totient Cayley graphs [2], so we will do the same for generalized totient graphs. We wish to acknowledge that the proofs of Lemma 5.1, Theorem 5.1, and Theorem 5.3 are inspired by proofs that Klotz and Sander used to establish similar results in the specific case when $R = \mathbb{Z}$.

Definition 5.1. For each prime ideal P of R and element s of R , define $\varepsilon(P, s)$ by

$$\varepsilon(P, s) = \begin{cases} 1, & \text{if } s \in P; \\ 2, & \text{if } s \notin P. \end{cases}$$

Let $I = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_t^{\alpha_t}$ be the (unique) factorization of I into a product of powers of distinct prime ideals. We define $F: R \rightarrow \mathbb{Z}$ by

$$F(s) = |R/I| \prod_{i=1}^t \left(1 - \frac{\varepsilon(P_i, s)}{|R/P_i|} \right).$$

The function F clearly depends on the choice of R and the choice of I , but we trust that this will not lead to confusion.

Lemma 5.1. *For any $a, b \in R$, the vertices $a + I$ and $b + I$ of $G_{R/I}$ have $F(a - b)$ common neighbors.*

Proof. As before, we will let $I = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_t^{\alpha_t}$ be the factorization of I into a product of powers of distinct prime ideals. Fix some $a, b \in R$, and note that a vertex $c + I$ is a common neighbor of $a + I$ and $b + I$ in $G_{R/I}$ if and only if $c - a \notin P_i$ and $c - b \notin P_i$ for all $i \in \{1, \dots, t\}$. For each $i \in \{1, \dots, t\}$, let N_i be the number of common neighbors of $a + P_i^{\alpha_i}$ and $b + P_i^{\alpha_i}$ in $G_{R/P_i^{\alpha_i}}$. It follows from the Chinese Remainder Theorem that the number of common neighbors of $a + I$ and $b + I$ in $G_{R/I}$ is $N_1 N_2 \cdots N_t$. Now, choose some $i \in \{1, \dots, t\}$ so that we may evaluate N_i . We use the natural homomorphism $\psi_i: R/P_i^{\alpha_i} \rightarrow R/P_i$ defined by $\psi_i: v + P_i^{\alpha_i} \mapsto v + P_i$, which we know is a k -to-1 mapping with $k = |R/P_i|^{\alpha_i - 1}$. A vertex $c + P_i^{\alpha_i}$ is a common neighbor of $a + P_i^{\alpha_i}$ and $b + P_i^{\alpha_i}$ in $G_{R/P_i^{\alpha_i}}$ if and only if $\psi_i(c + P_i^{\alpha_i}) \neq a + P_i$ and $\psi_i(c + P_i^{\alpha_i}) \neq b + P_i$. Therefore, if we wish to choose $c + P_i^{\alpha_i}$ to be a

common neighbor of $a + P_i^{\alpha_i}$ and $b + P_i^{\alpha_i}$ in $G_{R/P_i^{\alpha_i}}$, then there are exactly $\varepsilon(P_i, a - b)$ elements of R/P_i that cannot be the image of $c + P_i^\alpha$ under ψ_i . We see that $N_i = |R/P_i|^{\alpha_i-1}(|R/P_i| - \varepsilon(P_i, a - b)) = |R/P_i^{\alpha_i}| \left(1 - \frac{\varepsilon(P_i, a - b)}{|R/P_i|}\right)$. Hence,

$$N_1 N_2 \cdots N_t = \prod_{i=1}^t |R/P_i^{\alpha_i}| \left(1 - \frac{\varepsilon(P_i, a - b)}{|R/P_i|}\right) = F(a - b).$$

□

Theorem 5.1. *If I is a prime ideal of R , then $d(G_{R/I}) = 1$. If I is not a prime ideal of R and I has no prime ideal divisors of index 2, then $d(G_{R/I}) = 2$.*

Proof. If I is a prime ideal of R , then $G_{R/I}$ is a complete graph because R/I is a field. The first statement of the theorem then follows easily because the diameter of any complete graph with more than one vertex is 1.

Suppose I is not a prime ideal of R and I has no prime ideal divisors of index 2. Let P be a prime ideal divisor of I . As $I \subsetneq P$, we may choose some $p \in P$ with $p \notin I$. The vertices I and $p + I$ are distinct and nonadjacent. This implies that $d(G_{R/I}) \geq 2$. Now, for any $a, b \in R$, it is easy to see that $F(a - b) > 0$ because the index of each prime ideal divisor of I is at least 3. Hence, for any $a, b \in R$, the vertices $a + I$ and $b + I$ have a common neighbor. This implies that $d(G_{R/I}) = 2$.

□

Theorem 5.2. *Let m be a positive integer, and suppose that I has exactly m distinct prime ideal divisors of index 2 in R . Then $G_{R/I}$ has exactly 2^{m-1} disconnected components, and all such components are bipartite graphs that are isomorphic to each other and whose diameters are at most 3.*

Proof. For any vector $v \in \mathbb{F}_2^m$, we will let $[v]_i$ denote the i^{th} component of v . Let P_1, P_2, \dots, P_m be the prime ideal divisors of I of index 2. We define a function $T: R/I \rightarrow \mathbb{F}_2^m$ so that, for each $i \in \{1, 2, \dots, m\}$ and $a \in R$, we

have

$$[T(a + I)]_i = \begin{cases} 0, & \text{if } a \in P_i; \\ 1, & \text{if } a \notin P_i. \end{cases}$$

It is easy to verify that T is well-defined. If we write $T^{-1}(v) = \{V \in R/I : T(V) = v\}$, then the collection of sets $\{T^{-1}(v)\}_{v \in \mathbb{F}_2^m}$ forms a partition of R/I into 2^m subsets. Let $\mathbf{1}$ denote the vector in \mathbb{F}_2^m whose components are all 1's. It is easy to see that $T(V + W) = T(V) + T(W)$ for all $V, W \in R/I$. Furthermore, $U(R/I) \subseteq T^{-1}(\mathbf{1})$. Therefore, two vertices V and W of $G_{R/I}$ can only be adjacent if $T(V) = \mathbf{1} + T(W)$. In other words, for each $v \in \mathbb{F}_2^m$, the vertices in $T^{-1}(v)$ are only adjacent to vertices in $T^{-1}(\mathbf{1} + v)$. Let A be a set of 2^{m-1} vectors in \mathbb{F}_2^m with the property that $v \in A$ if and only if $\mathbf{1} + v \notin A$, and write $A = \{v_1, v_2, \dots, v_{2^{m-1}}\}$. For each $i \in \{1, 2, \dots, 2^{m-1}\}$, write $S_i = T^{-1}(v_i) \cup T^{-1}(\mathbf{1} + v_i)$, and let B_i be the subgraph of $G_{R/I}$ induced by S_i . Because no vertex in S_i is adjacent to any vertex in S_j when $i \neq j$, we see that $G_{R/I}$ is the union of the 2^{m-1} disconnected subgraphs $B_1, B_2, \dots, B_{2^{m-1}}$. Furthermore, each subgraph B_i is bipartite because we may partition the set of vertices of B_i into the sets $T^{-1}(v_i)$ and $T^{-1}(\mathbf{1} + v_i)$.

Choose some $k \in \{1, 2, \dots, 2^{m-1}\}$ and some $a+I, b+I \in T^{-1}(v_k)$. Observe that $T(a - b + I) = T(a + I) - T(b + I) = v_k - v_k = \mathbf{0}$, where $\mathbf{0}$ is the zero vector in \mathbb{F}_2^m . In other words $\varepsilon(P_i, a - b) = 1$ for all $i \in \{1, 2, \dots, m\}$. This implies that $F(a - b) > 0$, so Lemma 5.1 tells us that $a + I$ and $b + I$ have a common neighbor. The same argument shows that any two vertices in $T^{-1}(\mathbf{1} + v_k)$ must have a common neighbor. Therefore, the subgraph B_k is connected and has diameter at most 3. As k was arbitrary, this shows that each subgraph B_i is connected and has diameter at most 3. Finally, the subgraphs $B_1, B_2, \dots, B_{2^{m-1}}$ are isomorphic to each other because $G_{R/I}$ is symmetric by Theorem 4.1.

□

Theorem 5.1 gives the diameter of $G_{R/I}$ when I is not divisible by a prime ideal of index 2. When I is divisible by a prime ideal of index 2, Theorem 5.2 tells us that $G_{R/I}$ could be a union of several disconnected components. The following theorem determines the diameter of each component of $G_{R/I}$ when I is divisible by a prime ideal of index 2.

Theorem 5.3. *Let m be a positive integer. Suppose $I = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_m^{\alpha_m} J$, where P_1, P_2, \dots, P_m are distinct prime ideals of index 2 in R , $\alpha_1, \alpha_2, \dots, \alpha_m$ are positive integers, and J is an ideal of R that is not divisible by a prime ideal of index 2. If $J = R$ and $\alpha_i = 1$ for all $i \in \{1, 2, \dots, m\}$, then the diameter of each component of $G_{R/I}$ is 1. If $J = R$ and $\alpha_i > 1$ for some $i \in \{1, 2, \dots, m\}$, then the diameter of each component of $G_{R/I}$ is 2. If $J \neq R$, then the diameter of each component of $G_{R/I}$ is 3.*

Proof. Preserve the notation from the proof of Theorem 5.2, and let $\lambda = \alpha_1 + \alpha_2 + \dots + \alpha_m$. First, suppose that $J = R$. The number of vertices in $G_{R/I}$ is $|R/I| = \prod_{i=1}^m |R/P_i|^{\alpha_i} = 2^\lambda$. We know from the proof of Theorem 5.2 that $T^{-1}(v_1)$ and $T^{-1}(\mathbf{1} + v_1)$ form two parts of the bipartite component B_1 . If $a + I \in T^{-1}(v_1)$ and $b + I \in T^{-1}(\mathbf{1} + v_1)$, then $T(b - a + I) = T(b + I) - T(a + I) = (\mathbf{1} + v_1) - v_1 = \mathbf{1}$. This implies that $b - a \notin P_i$ for all $i \in \{1, 2, \dots, m\}$, so $a + I$ and $b + I$ are adjacent. This shows that B_1 is a complete bipartite graph. Theorem 5.2 tells us that $G_{R/I}$ has 2^{m-1} disconnected components that are all isomorphic to each other, so B_1 must contain exactly $\frac{2^\lambda}{2^{m-1}} = 2^{\lambda-m+1}$ vertices. If $\alpha_i = 1$ for all $i \in \{1, 2, \dots, m\}$, then B_1 has only two vertices. In this case, the diameter of B_1 is 1 because B_1 is isomorphic to the complete bipartite graph $K_{1,1}$. If $\alpha_i > 1$ for some $i \in \{1, \dots, m\}$, then $\lambda > m$. In this case, B_1 is a complete bipartite graph with at least four vertices, so it must have diameter 2. Because all of the components of $G_{R/I}$ are isomorphic to B_1 , this completes the proof of the case in which $J = R$. Suppose, now, that $J \neq R$. The Chinese Remainder Theorem guarantees that we may choose some $y \in J$ such that $y \notin P_i$ for all $i \in \{1, 2, \dots, m\}$. There exists some $\ell \in \{1, 2, \dots, 2^{m-1}\}$ such that $S_\ell = T^{-1}(\mathbf{0}) \cup T^{-1}(\mathbf{1})$. Because $T(I) = \mathbf{0}$ and $T(y + I) = \mathbf{1}$, we know that I and $y + I$ are in the same component B_ℓ . The vertices I and $y + I$ are not adjacent because $y \in J \neq R$. Also, Lemma 5.1 implies that I and $y + I$ have no common neighbors because $\varepsilon(P_1, y) = 2$. Hence, the diameter of B_ℓ is at least 3. By Theorem 5.2, the diameter of B_ℓ must be equal to 3. The proof then follows from the fact that all components of $G_{R/I}$ are isomorphic to B_ℓ . \square

6 Strong Colorings of Generalized Totient Graphs

Suppose we are given a positive integer k and a graph G with n vertices. Let ℓ be the least nonnegative integer such that $k|\ell + n$, and let H be the graph that results from adding ℓ isolated vertices to G . We say that G is strongly k -colorable if, for any given partition of the vertices of H into subsets of size k , it is possible to properly color the vertices of H so that each color appears exactly once in each subset of the partition. Observe that if G is simple and has some vertex v of degree at least k , then we can choose to partition the vertices of H into subsets of size k so that one of the subsets is contained in the neighborhood of v . As no vertex in the neighborhood of v can have the same color as v in a proper coloring of H , we see that any simple graph with a vertex of degree at least k cannot be strongly k -colorable. The strong chromatic number of a graph G , denoted $s\chi(G)$, is the smallest positive integer k such that G is strongly k -colorable. It follows from the preceding discussion that $s\chi(G)$ must be greater than $\Delta(G)$ if G is simple.

We say that an edge-coloring of a graph is strong if any two distinct edges with adjacent endpoints are colored differently. The strong chromatic index of a graph G , denoted $s'(G)$, is the smallest positive integer r such that it is possible to strongly edge-color G with r colors.

In this section, we briefly study the strong chromatic numbers and strong chromatic indices of some generalized totient graphs.

Theorem 6.1. *Let P be a nonzero prime ideal of R such that R/P is finite, and let α be a positive integer. Then $s\chi(G_{R/P^\alpha}) = |R/P|^\alpha$.*

Proof. For convenience, we will write $y = |R/P|$. Note that G_{R/P^α} has y^α vertices. We know that $s\chi(G_{R/P^\alpha}) > \Delta(G_{R/P^\alpha}) = \varphi(R/P^\alpha)$, and Theorem 2.2 tells us that $\varphi(R/P^\alpha) = y^\alpha - y^{\alpha-1}$. Let $k = y^\alpha - y^{\alpha-1} + m$ for some positive integer $m < y^{\alpha-1}$, and assume by way of contradiction that G_{R/P^α} is strongly k -colorable. It is easy to see that $\ell = 2k - y^\alpha$ is the least nonnegative integer such that $\ell + y^\alpha$ is divisible by k . Let H be the graph that results from adding ℓ isolated vertices v_1, v_2, \dots, v_ℓ to G_{R/P^α} . Let $A = \{v + P^\alpha \in R/P^\alpha : v \in P\}$, and let $B = \{v_1, v_2, \dots, v_r\}$, where $r = k - y^{\alpha-1} = y^\alpha - 2y^{\alpha-1} + m$. Then

$|A \cup B| = k$ because $|A| = y^{\alpha-1}$. If we let C be the set of k vertices of H that are not in $A \cup B$, then we see that the two sets $A \cup B$ and C form a partition of the set of vertices of H into subsets of size k . Therefore, because G_{R/P^α} is strongly k -colorable, it is possible to properly color the vertices of H so that each color appears exactly once in $A \cup B$ and exactly once in C . Let $s + P^\alpha \in A$ be colored with the color c . We know that c must be used to color exactly one vertex $V \in C$. Suppose $V = u + P^\alpha \in G_{R/P^\alpha}$. Then $u \notin P$ because $V \notin A$. However, $s \in P$, so $s - u \notin P$. This shows that $s - u + P^\alpha \in U(R/P^\alpha)$, so V is adjacent to $s + P^\alpha$. This is a contradiction because we assumed the coloring to be proper. Thus, each of the $y^{\alpha-1}$ colors used to color the elements of A must be used to color one of the elements of the set $D = \{v_{r+1}, v_{r+2}, \dots, v_\ell\}$. However, this is impossible because $|D| = \ell - r = 2k - y^\alpha - (y^\alpha - 2y^{\alpha-1} + m) = 2(y^\alpha - y^{\alpha-1} + m) - y^\alpha - (y^\alpha - 2y^{\alpha-1} + m) = m < y^{\alpha-1}$. Hence, we must have $s\chi(G_{R/P^\alpha}) \geq y^\alpha$. Clearly, G_{R/P^α} is strongly y^α -colorable, so $s\chi(G_{R/P^\alpha}) = y^\alpha = |R/P|^\alpha$. \square

Theorem 6.2. *Let P , Q , and M be nonzero ideals of R such that P and Q are prime, $M \not\subseteq Q$, R/P and R/M are finite and nontrivial, and $|R/Q| = 2$. Let α be a positive integer. We have*

$$s'(G_{R/P^\alpha}) = \frac{1}{2}|R/P|^\alpha \varphi(R/P^\alpha) = \frac{1}{2}|R/P|^{2\alpha-1}(|R/P| - 1)$$

and

$$s'(G_{R/QM}) \leq \frac{1}{2}|R/M| \varphi(R/M).$$

Proof. By Theorem 4.5, any two adjacent vertices of G_{R/P^α} dominate G_{R/P^α} . Therefore, in any strong edge-coloring of G_{R/P^α} , no two distinct edges can have the same color. This means that any strong edge-coloring of G_{R/P^α} must use exactly $\frac{1}{2}|R/P|^\alpha \varphi(R/P^\alpha)$ colors because G_{R/P^α} has $\frac{1}{2}|R/P|^\alpha \varphi(R/P^\alpha)$ edges.

Because there are only two cosets of Q in R and $1 \notin Q$, the two cosets of Q in R must be Q and $1 + Q$. Therefore, if we define the element $2 = 1 + 1$ of R (it is possible that $2 = 0$), then it follows from the fact that $1 \notin Q$ that $2 + Q \neq 1 + Q$. Therefore, $2 + Q = Q$, so $2 \in Q$. Now, consider the graph $G_{R/QM}$, which has an edge set of size

$$\frac{1}{2}|R/QM| \varphi(R/QM) = \frac{1}{2}|R/Q| \cdot |R/M| \varphi(R/Q) \varphi(R/M) = |R/M| \varphi(R/M).$$

Choose some $\mu \in M$ with $\mu \notin Q$. For any vertex $v + QM$ of $G_{R/QM}$, let $f(v + QM) = v + \mu + QM$. For any edge $\{Y, Z\}$ of $G_{R/QM}$, let $h(\{Y, Z\}) = \{f(Y), f(Z)\}$. That is, the function h maps an edge connecting the vertices Y and Z to the edge connecting the vertices $f(Y)$ and $f(Z)$. Notice that, for any vertex Y of $G_{R/QM}$, we have $f(f(Y)) = Y$ because $2\mu \in QM$. Furthermore, it is easy to see that $f(Y)$ is not equal to Y or adjacent to Y . This shows that $h(h(E)) = E \neq h(E)$ for all edges E of $G_{R/QM}$. Let us color the edges of $G_{R/QM}$ so that two distinct edges e_1 and e_2 have the same color if and only if $e_2 = h(e_1)$. Because each color is used to color two of the $|R/M|\varphi(R/M)$ edges of $G_{R/QM}$, we see that this coloring uses $\frac{1}{2}|R/M|\varphi(R/M)$ colors. To show that this coloring is strong, suppose $a + QM$ and $b + QM$ are adjacent vertices of $G_{R/QM}$. We stated already that $a + QM$ is not adjacent to $f(a + QM)$. Because $\mu \notin Q$ and $a - b \notin Q$, we must have $\mu + Q = a - b + Q = 1 + Q$. Therefore, $a - [b + \mu] \in Q$, which means that $a + QM - f(b + QM) \notin U(R/QM)$. Hence, $a + QM$ is not adjacent to $f(b + QM)$. By the same token, $b + QM$ is not adjacent to $f(a + QM)$ or $f(b + QM)$. This shows that, for any edge E , the only other edge with the same color as E cannot have an endpoint adjacent to an endpoint of E . Thus, the coloring is strong, so the result follows. \square

7 Erratum

We use this section to briefly expose a counterexample to Theorem 4.3 of a paper of Manjuri and Maheswari [5]. We hope to encourage the reader to discover a correct solution to this interesting problem and perhaps even generalize the solution in order to solve an analogous problem concerning generalized totient graphs. The theorem states that if a composite integer n is not twice a prime, then the strong domination number of the Euler totient Cayley graph $G_{\mathbb{Z}/(n)}$ is $\lambda + 1$, where λ is the length of the longest string of consecutive integers that each have a prime factor in common with n . It is apparent from the definition that Manjuri and Maheswari give for the strong domination number of a graph that the strong domination number of any regular graph G is simply the minimum number of vertices of G that form a set that dominates G . For example, because $G_{\mathbb{Z}/(30)}$ is a regular graph and the set of five vertices $\{\overline{0}, \overline{7}, \overline{10}, \overline{12}, \overline{15}\}$ dominates $G_{\mathbb{Z}/(30)}$ (we let \overline{k} denote

the vertex $k + (30)$, the strong domination number of $G_{\mathbb{Z}/(30)}$ must be less than or equal to 5. However, the length of the longest string of consecutive integers that each have a prime factor in common with 30 is $\lambda = 5$ (e.g., 2, 3, 4, 5, 6). Hence, the theorem states that the strong domination number of $G_{\mathbb{Z}/(n)}$ is 6, which is false.

8 Concluding Remarks

We wish to acknowledge the potential to generalize and strengthen the preceding results. For example, one might wish to study the infinite graphs that arise from eliminating the restriction that R/I be finite. Alternatively, one might attempt to gather information about analogues of gcd-graphs [2] in Dedekind domains. There is certainly room for strengthening Theorems 6.1 and 6.2, which only apply to generalized totient graphs with specific properties. Theorem 4.6 leads us to inquire about which generalized totient graphs have girths not equal to 3 or 4. Finally, we note that we have obviously not exhausted all of the graph parameters of generalized totient graphs that one might wish to study. For instance, we have not considered any of the many fascinating graph parameters associated with games such as pebbling and the chip-firing game.

9 Acknowledgements

Dedicated to my wonderful and inspiring parents, Marc and Susan Defant.

References

- [1] Dejter, I. J., and Giudici, R. E. On unitary Cayley graphs. *J. Combin. Math. Combin. Comput.* 18 (1995), 121124.
- [2] Klotz, Walter; Sander, Torsten. Some properties of unitary Cayley graphs. *Electron. J. Combin.* (2007).

- [3] Madhavi, Levaku; Maheswari, Bommireddy. Enumeration of Hamilton cycles and triangles in Euler totient Cayley graphs. *Graph Theory Notes* N. Y. 59 (2010), 28–31.
- [4] Maheswari, B., Manjuri, M. Clique dominating sets of Euler totient Cayley graphs. *IOSR Journal of Mathematics* (2013), 46–49.
- [5] Maheswari, B., Manjuri, M. Strong dominating sets of some arithmetic graphs, *International Journal of Computer Applications (IJCA)*, Volume 83, No3 (2013), 36–40.
- [6] V. Schemmel, Über relative Primzahlen, *Journal für die reine und angewandte Mathematik*, 70 (1869), 191–192.